VYKONÁVACIE ROZHODNUTIE KOMISIE (EÚ) 2021/1073

z 28. júna 2021,

ktorým sa stanovujú technické špecifikácie a pravidlá pre vykonávanie rámca dôvery pre digitálny COVID preukaz EÚ zriadený nariadením Európskeho parlamentu a Rady (EÚ) 2021/953

(Text s významom pre EHP)

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) 2021/953 ([1]), a najmä na jeho článok 9 ods. 1 a 3,

keďže:

(1) V nariadení (EÚ) 2021/953 sa stanovuje digitálny COVID preukaz EÚ, ktorý má slúžiť ako dôkaz, že osoba dostala vakcínu proti ochoreniu COVID-19, má negatívny výsledok testu alebo prekonala infekciu.

(2) Na to, aby digitálny COVID preukaz EÚ bolo možné používať v celej Únii, je potrebné stanoviť technické špecifikácie a pravidlá na vypĺňanie, bezpečné vystavovanie a overovanie digitálnych COVID preukazov, zabezpečenie ochrany osobných údajov, stanovenie spoločnej štruktúry jedinečného identifikátora potvrdenia a vystavovanie platného, zabezpečeného a interoperabilného čiarového kódu. Daným rámcom dôvery sa stanovuje aj prostredie pre zabezpečenie interoperability s medzinárodnými normami a technologickými systémami, pričom tento rámec by ako taký mohol predstavovať vzor pre globálnu spoluprácu.

(3) Z hľadiska schopnosti čítať a interpretovať digitálny COVID preukaz EÚ sa vyžaduje spoločná štruktúra údajov a dohoda o zamýšľanom význame jednotlivých dátových polí nosného obsahu a ich možných hodnôt. V záujme tejto interoperability treba vymedziť spoločnú koordinovanú štruktúru údajov pre rámec digitálneho COVID preukazu EÚ. Usmernenia pre tento rámec boli vytvorené v rámci siete elektronického zdravotníctva, ktorá bola zriadená na základe smernice Európskeho parlamentu a Rady 2011/24/EÚ ([2]). Tieto usmernenia by sa mali zohľadniť pri stanovení technických špecifikácií, ktorými sa určuje formát a správa dôveryhodnosti digitálneho COVID preukazu EÚ. Mala by sa určiť špecifikácia pre štruktúru údajov a mechanizmy kódovania, ako aj transportný mechanizmus kódovania v strojovo čitateľnom optickom formáte (QR), ktorý umožňuje zobrazenie na obrazovke mobilného zariadenia alebo tlač na papier.

(4) Okrem technických špecifikácií v súvislosti s formátom a správou dôveryhodnosti digitálneho COVID preukazu EÚ by sa mali stanoviť všeobecné pravidlá na účely vypĺňania potvrdení, ktoré sa majú použiť pre kódované hodnoty v obsahu digitálneho COVID preukazu EÚ. Komisia by mala pravidelne aktualizovať a zverejňovať súbory hodnôt, ktorými sa dané pravidlá vykonávajú, a to na základe relevantnej činnosti siete elektronického zdravotníctva.

(5) Podľa nariadenia (EÚ) 2021/953 pravé potvrdenia, ktoré tvoria digitálny COVID preukaz EÚ, majú byť jednotlivo identifikovateľné pomocou jedinečného identifikátora potvrdenia, pričom treba zohľadniť, že občanom sa môže vystaviť viac ako jedno potvrdenie počas obdobia účinnosti nariadenia (EÚ) 2021/953. Jedinečný identifikátor potvrdenia má pozostávať z alfanumerického radu a členské štáty by mali zabezpečiť, aby neobsahoval žiadne údaje, ktoré by ho spájali s inými dokladmi alebo identifikátormi, ako sú čísla pasu alebo preukazu totožnosti, aby sa predišlo možnej identifikácii držiteľa. S cieľom zabezpečiť, že identifikátor potvrdenia bude jedinečný, sa majú určiť technické špecifikácie a pravidlá pre jeho spoločnú štruktúru.

([1]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/953 zo 14. júna 2021 o rámci pre vydávanie, overovanie a uznávanie interoperabilných potvrdení o očkovaní proti ochoreniu COVID-19, o vykonaní testu a prekonaní tohto ochorenia (digitálny COVID preukaz EÚ) s cieľom uľahčiť voľný pohyb počas pandémie ochorenia COVID-19 (Ú. v. EÚ L 211, 15.6.2021, s. 1).

([2]) Smernica Európskeho parlamentu a Rady 2011/24/EÚ z 9. marca 2011 o uplatňovaní práv pacientov pri cezhraničnej zdravotnej starostlivosti (Ú. v. EÚ L 88, 4.4.2011, s. 45).

(6) Bezpečnosť, pravosť, platnosť a integrita potvrdení, ktoré tvoria digitálny COVID preukaz EÚ, a ich súlad s právom Únie v oblasti ochrany údajov sú kľúčom k ich uznávaniu vo všetkých členských štátoch. Tieto ciele sa dosahujú prostredníctvom rámca dôvery, v ktorom sa stanovia pravidlá a infraštruktúra pre spoľahlivé a bezpečné vydávanie a overovanie digitálnych COVID preukazov EÚ. Rámec dôvery by mal byť okrem iného založený na infraštruktúre verejných kľúčov s reťazcom dôvery siahajúcim od zdravotníckych alebo iných dôveryhodných orgánov členských štátov až po jednotlivé subjekty vydávajúce digitálne COVID preukazy EÚ. S cieľom zabezpečiť systém interoperability pre celú EÚ preto Komisia zriadila centrálny systém – bránu digitálneho COVID preukaz EÚ (ďalej len „brána“) –, v ktorej sa ukladajú verejné kľúče použité na overovanie. Keď sa naskenuje potvrdenie s kódom QR, digitálny podpis sa overí pomocou príslušného verejného kľúča, ktorý sa už skôr uložil v tejto centrálnej bráne. Na zabezpečenie integrity a pravosti údajov možno použiť digitálne podpisy. Infraštruktúry verejných kľúčov zabezpečujú dôveru prepojením verejných kľúčov s vystaviteľmi potvrdení. V rámci brány sa v záujme zabezpečenia pravosti využívajú viaceré certifikáty verejného kľúča. S cieľom zaistiť zabezpečenú výmenu údajov medzi členskými štátmi, pokiaľ ide o materiál verejných kľúčov, a umožniť širokú interoperabilitu je potrebné zriadiť certifikáty verejného kľúča, ktoré možno používať, a určiť spôsob ich generovania.

(7) Toto rozhodnutie umožňuje vykonávanie požiadaviek nariadenia (EÚ) 2021/953 tak, aby sa obmedzilo spracovanie osobných údajov na minimálnu mieru potrebnú na funkčnosť digitálneho COVID preukazu EÚ, a prispieva k vykonávaniu zo strany konečných prevádzkovateľov rešpektujúc špecificky navrhnutú ochranu údajov.

(8) V súlade s nariadením (EÚ) 2021/953 sa orgány alebo iné určené subjekty zodpovedné za vydávanie potvrdení považujú za prevádzkovateľov v zmysle článku 4 bodu 7 nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 ([3]), v rámci ich úlohy spracúvania osobných údajov v procese vystavovania. V závislosti od toho, ako členské štáty organizujú postup vydávania, môže existovať jeden alebo viacero orgánov alebo určených subjektov – napríklad regionálne služby zdravotnej starostlivosti. V súlade so zásadou subsidiarity o tom rozhodujú členské štáty. V prípade viacerých orgánov alebo iných určených subjektov majú preto členské štáty najlepšie predpoklady zabezpečiť, aby ich príslušné zodpovednosti boli jednoznačne rozdelené, a to nezávisle od toho, či predstavujú samostatných alebo spoločných prevádzkovateľov (vrátane regionálnych služieb zdravotnej starostlivosti, ktoré zriadia spoločný portál pre pacientov na vydávanie potvrdení). Podobne, pokiaľ ide o overovanie potvrdení príslušnými orgánmi členského štátu určenia alebo tranzitu alebo prevádzkovateľmi služieb cezhraničnej osobnej dopravy, od ktorých sa podľa vnútroštátneho práva vyžaduje vykonávanie určitých opatrení v oblasti verejného zdravia počas pandémie ochorenia COVID-19, títo overovatelia musia konať v súlade s povinnosťami vyplývajúcimi z pravidiel ochrany údajov.

(9) Prostredníctvom brány digitálneho COVID preukazu EÚ sa osobné údaje nespracúvajú, keďže brána obsahuje len verejné kľúče podpisových autorít. Tieto kľúče sa vzťahujú na podpisové autority a neumožňujú priamu ani nepriamu opätovnú identifikáciu fyzickej osoby, ktorej bolo vystavené potvrdenie. Komisia by tak v rámci svojej úlohy správcu brány nemala byť prevádzkovateľom ani sprostredkovateľom osobných údajov.

(10) V súlade s článkom 42 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725 ([4]) sa uskutočnili konzultácie s európskym dozorným úradníkom pre ochranu údajov, ktorý vydal stanovisko 22. júna 2021.

(11) Vzhľadom na to, že technické špecifikácie a pravidlá sú potrebné na uplatňovanie nariadenia (EÚ) 2021/953 od 1. júla 2021, okamžité uplatňovanie tohto rozhodnutia je odôvodnené.

(12) Preto vzhľadom na potrebu rýchleho zavedenia digitálneho COVID preukazu EÚ by toto rozhodnutie malo nadobudnúť účinnosť dňom jeho zverejnenia,

([3]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1).

([4]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018, s. 39).

PRIJALA TOTO ROZHODNUTIE:

Článok 1

Technické špecifikácie pre digitálny COVID preukaz EÚ, ktorými sa stanovuje generická štruktúra údajov, mechanizmy kódovania a transportný mechanizmus kódovania v strojovo čitateľnom optickom formáte, sa uvádzajú v prílohe I.

Článok 2

Pravidlá vypĺňania potvrdení uvedených v článku 3 ods. 1 nariadenia (EÚ) 2021/953 sa uvádzajú v prílohe II k tomuto rozhodnutiu.

Článok 3

Požiadavky, ktorými sa stanovuje spoločná štruktúra jedinečného identifikátora potvrdenia, sa uvádzajú v prílohe III.

Článok 4

Pravidlá správy certifikátov verejného kľúča v súvislosti s bránou digitálneho COVID preukazu EÚ, ktorými sa podporujú aspekty interoperability rámca dôvery, sa uvádzajú v prílohe IV.

Toto rozhodnutie nadobúda účinnosť dňom jeho uverejnenia v *Úradnom vestníku Európskej únie*.

V Bruseli 28. júna 2021

Za Komisiu
predsedníčka
Ursula VON DER LEYEN

PRÍLOHA I

FORMÁT A SPRÁVA DÔVERYHODNOSTI

Generická štruktúra údajov, mechanizmy kódovania a transportný mechanizmus kódovania v strojovo čitateľnom optickom formáte (ďalej len „QR“)

1. Úvod

V technických špecifikáciách stanovených v tejto prílohe sa uvádza generická štruktúra údajov a mechanizmy kódovania pre digitálny COVID preukaz EÚ. Určuje sa v nich aj transportný mechanizmus kódovania v strojovo čitateľnom optickom formáte („QR“), ktorý možno zobraziť na obrazovke mobilného zariadenia alebo vytlačiť. Formáty kontajnera elektronického zdravotného potvrdenia v týchto špecifikáciách sú generické, v tomto kontexte však slúžia na prenos digitálneho COVID preukazu EÚ.

2. Terminológia

Na účely tejto prílohy sú „vystavitelia“ organizácie, ktoré používajú tieto špecifikácie na vystavovanie zdravotných potvrdení, a „overovatelia“ sú organizácie, ktoré uznávajú zdravotné potvrdenia ako dôkaz o zdravotnom stave. „Účastníci“ sú vystavitelia a overovatelia. V prípade niektorých aspektov stanovených v tejto prílohe sa vyžaduje koordinácia medzi účastníkmi, napríklad pokiaľ ide o správu priestoru názvov a distribúciu kryptografických kľúčov. Predpokladá sa, že tieto úlohy vykonáva strana, ktorá sa ďalej označuje ako „sekretariát“.

3. Formát kontajnera elektronického zdravotného potvrdenia

Formát kontajnera elektronického zdravotného potvrdenia (ďalej len „HCERT“) slúži ako jednotný a štandardizovaný prenosový prostriedok pre zdravotné potvrdenia od rôznych vystaviteľov. Cieľom týchto špecifikácií je harmonizovať spôsob zobrazovania, kódovania a podpisovania zdravotných potvrdení, aby sa uľahčila interoperabilita.

Z hľadiska schopnosti čítať a interpretovať digitálny COVID preukaz EÚ vystavený ktorýmkoľvek vystaviteľom sa vyžaduje spoločná štruktúra údajov a dohoda o význame jednotlivých dátových polí nosného obsahu. S cieľom uľahčiť takúto interoperabilitu sa spoločná koordinovaná štruktúra údajov vymedzuje pomocou schémy „JSON“, ktorá tvorí rámec digitálneho COVID preukazu EÚ.

3.1. *Štruktúra nosného obsahu*

Nosný obsah je štruktúrovaný a kódovaný vo formáte CBOR s digitálnym podpisom COSE. Tento formát sa bežne označuje ako „webový token CBOR“ (ďalej len „CWT“) a je vymedzený v dokumente RFC 8392 ([1]). Nosný obsah vymedzený v ďalších oddieloch sa transportuje v rámci deklarácie hcert.

Overovateľ musí mať možnosť overiť integritu a pravosť pôvodu nosného obsahu. Na poskytnutie tohto mechanizmu musí vystaviteľ podpísať CWT pomocou schémy asymetrického elektronického podpisu, ako sa vymedzuje v špecifikácii COSE (RFC 8152 ([2])).

3.2. *Hodnoty CWT*

3.2.1. Prehľad štruktúry CWT

Chránené záhlavie

— Algoritmus podpisu (alg, označenie 1)

— Identifikátor kľúča (kid, označenie 4)

Nosný obsah

— Vystaviteľ (iss, kľúč deklarácie 1, voliteľné, kód vystaviteľa podľa normy ISO 3166-1 alpha-2)

— Čas vystavenia (iat, kľúč deklarácie 6)

— Čas exspirácie (exp, kľúč deklarácie 4)

— Zdravotné potvrdenie (hcert, kľúč deklarácie -260)

— Digitálny COVID preukaz EÚ v. 1 (eu_DCC_v1, kľúč deklarácie 1)

Podpis

([1]) rfc8392 (ietf.org).
([2]) rfc8152 (ietf.org).

3.2.2. Algoritmus podpisu

Parameter algoritmu podpisu (alg) označuje, aký algoritmus slúži na vytvorenie podpisu. Musí spĺňať alebo prekračovať aktuálne usmernenia organizácie SOG-IS, ktorých súhrn je uvedený v ďalších odsekoch.

Je vymedzený jeden primárny a jeden sekundárny algoritmus. Sekundárny algoritmus sa má použiť, len ak primárny algoritmus nie je prijateľný v rámci pravidiel a predpisov, ktoré sa vzťahujú na vystaviteľa.

S cieľom zaistiť zabezpečenie systému musia všetky implementácie zahŕňať sekundárny algoritmus. Z tohto dôvodu sa musí zaviesť primárny aj sekundárny algoritmus.

Pre primárny a sekundárny algoritmus platia tieto úrovne stanovené SOG-IS:

— Primárny algoritmus: primárny algoritmus je algoritmus pre digitálny podpis na báze eliptických kriviek (ECDSA), ako sa vymedzuje v oddiele 2.3 (normy ISO/IEC 14888-3:2006), s využitím parametrov P-256, ako sa vymedzujú v dodatku D (D.1.2.3) k (norme FIPS PUB 186-4), v kombinácii s hašovacím algoritmom SHA-256, ako sa vymedzuje v rámci funkcie 4 (normy ISO/IEC 10118-3:2004).

Zodpovedá to parametru ES256 algoritmu COSE.

— Sekundárny algoritmus: sekundárny algoritmus je RSASSA-PSS, ako sa vymedzuje v dokumente (RFC 8230 ([3])), s modulom 2048 bitov v kombinácii s hašovacím algoritmom SHA-256, ako sa vymedzuje v rámci funkcie 4 (normy ISO/IEC 10118–3:2004).

V rámci algoritmu COSE to zodpovedá parametru: PS256.

3.2.3. Identifikátor kľúča

Deklarácia identifikátora kľúča (kid) označuje certifikát podpisovateľa dokumentov (DSC) obsahujúci verejný kľúč, ktorý má overovateľ použiť na kontrolu správnosti digitálneho podpisu. Správa certifikátov verejného kľúča vrátane požiadaviek na DSC je opísaná v prílohe IV.

Deklaráciu identifikátora kľúča (kid) používajú overovatelia na výber správneho verejného kľúča zo zoznamu kľúčov vzťahujúcich sa na vystaviteľa, ako určuje deklarácia vystaviteľa (iss). Vystaviteľ môže používať súčasne viacero kľúčov, a to z administratívnych dôvodov alebo pri aktualizácii kľúčov. Pole identifikátora kľúča nie je kritické z hľadiska bezpečnosti. Môže sa preto v prípade potreby nachádzať v nechránenom záhlaví. Overovatelia musia akceptovať obe možnosti. Ak sú prítomné obe možnosti, musí sa použiť identifikátor kľúča v chránenom záhlaví.

Vzhľadom na skrátenie identifikátora (kvôli veľkostným obmedzeniam) existuje malá, nie však nulová pravdepodobnosť, že celkový zoznam podpisových certifikátov dokumentu (ďalej len „certifikát DSC“), ktoré overovateľ akceptuje, môže obsahovať certifikáty DSC s duplicitnými identifikátormi kid. Z tohto dôvodu musí overovateľ skontrolovať všetky podpisové certifikáty dokumentu s daným identifikátorom kid.

3.2.4. Vystaviteľ

Deklarácia vystaviteľa (iss) je hodnota reťazca, v ktorom sa voliteľne môže uvádzať kód krajiny podľa normy ISO 3166-1 alpha-2 vzťahujúci sa na subjekt, ktorý vystavuje zdravotné potvrdenie. Pomocou tejto deklarácie môže overovateľ identifikovať, ktorá množina certifikátov DSC sa má použiť na overenie. Na identifikáciu tejto deklarácie slúži kľúč deklarácie 1.

3.2.5. Čas exspirácie

Deklarácia času exspirácie (exp) musí obsahovať časovú pečiatku v celočíselnom formáte NumericDate (ako sa uvádza v časti 2 dokumentu RFC 8392 ([4])), ktorou sa uvádza, po aký čas sa má tento konkrétny podpis nosného obsahu považovať za platný, pričom po uplynutí toho času musí overovateľ odmietnuť nosný obsah z dôvodu uplynutia jeho platnosti. Účelom parametra exspirácie je vynútiť obmedzenie obdobia platnosti zdravotného potvrdenia. Na identifikáciu tejto hodnoty slúži kľúč deklarácie 4.

Čas exspirácie nesmie presiahnuť obdobie platnosti certifikátu DSC.

([3]) rfc8230 (ietf.org).
([4]) rfc8392 (ietf.org).

3.2.6. Čas vystavenia

Deklarácia času vystavenia (iat) musí obsahovať časovú pečiatku v celočíselnom formáte NumericDate (ako sa uvádza v časti 2 dokumentu RFC 8392 ([5])), ktorou sa uvádza čas vytvorenia zdravotného potvrdenia.

V poli Čas vystavenia sa nesmie uvádzať čas pred obdobím platnosti certifikátu DSC.

Overovatelia môžu uplatňovať dodatočné politiky, ktorých účelom je obmedzenie platnosti zdravotného potvrdenia na základe času vystavenia. Na identifikáciu tejto hodnoty slúži kľúč deklarácie 6.

3.2.7. Deklarácia zdravotného potvrdenia

Deklarácia zdravotného potvrdenia (hcert) je objekt JSON (RFC 7159 ([6])), ktorý obsahuje informácie o zdravotnom stave. V rámci rovnakej deklarácie môže existovať niekoľko rôznych druhov zdravotných potvrdení, z ktorých jedno je digitálny COVID preukaz EÚ.

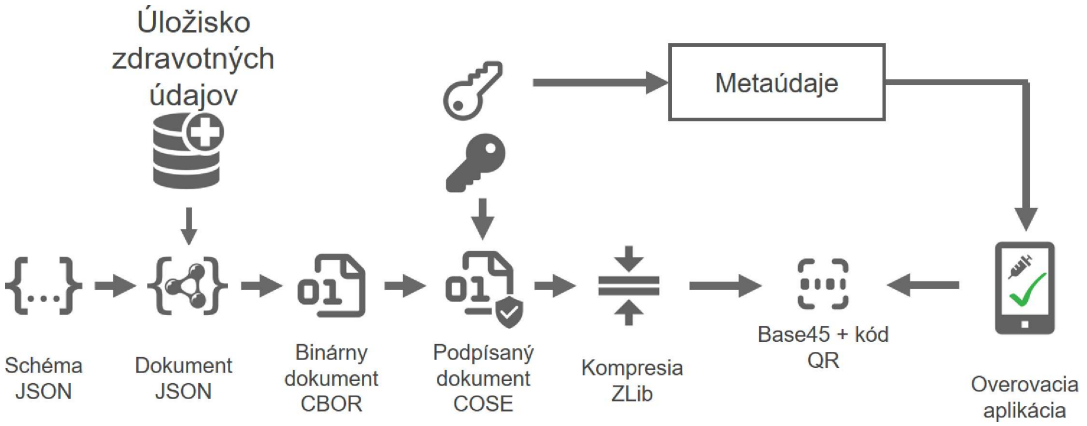
Formát JSON slúži výlučne na účely schémy. Zobrazovací formát je CBOR, ako sa vymedzuje v dokumente (RFC 7049 ([7])). Vývojári aplikácií v skutočnosti vôbec nemusia vykonávať dekódovanie alebo kódovanie do formátu JSON alebo z neho, ale môžu používať príslušnú štruktúru v pamäti.

Na identifikáciu tejto deklarácie slúži kľúč deklarácie -260.

Reťazce v objekte JSON by sa mali normalizovať podľa normalizačnej formy s kanonickým zložením (NFC) vymedzenej v norme Unicode. V dekódovacích aplikáciách by sa však mal pri týchto aspektoch uplatňovať permisívny a robustný prístup a dôrazne sa odporúča akceptovanie akéhokoľvek primeraného druhu konverzie. Ak sa počas dekódovania alebo v rámci následných porovnávacích funkcií zistia údaje, ktoré nie sú normalizované, pri implementáciách by sa malo postupovať tak, akoby bol vstup normalizovaný metódou NFC.

4. Serializácia a vytvorenie nosného obsahu digitálneho COVID preukazu EÚ

Ako vzor serializácie slúži táto schéma:



Proces sa začína extrakciou údajov napríklad z úložiska zdravotných údajov (alebo z externého zdroja údajov), pričom sa na tieto extrahované údaje uplatní štruktúra podľa vymedzených schém digitálneho COVID preukazu EÚ. V tomto procese sa pred tým, ako začne serializácia na formát CBOR, môže uskutočniť konverzia na vymedzený formát údajov a transformácia na účely ľudskej čitateľnosti. Skratky deklarácií sa v každom prípade priradia zobrazovaným názvom pred serializáciou a po deserializácii.

Voliteľný vnútroštátny obsah údajov nie je povolený v potvrdeniach vystavených podľa nariadenia (EÚ) 2021/953 ([8]). Obsah údajov je obmedzený na vymedzené dátové prvky v minimálnom súbore údajov, ktorý je určený v prílohe k nariadeniu (EÚ) 2021/953.

([5]) rfc8392 (ietf.org).
([6]) rfc7159 (ietf.org).
([7]) rfc7049 (ietf.org).
([8]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/953 zo 14. júna 2021 o rámci pre vydávanie, overovanie a uznávanie interoperabilných potvrdení o očkovaní proti ochoreniu COVID-19, o vykonaní testu a prekonaní tohto ochorenia (digitálny COVID preukaz EÚ) s cieľom uľahčiť voľný pohyb počas pandémie ochorenia COVID-19 (Ú. v. EÚ L 211, 15.6.2021, s. 1).

5. **Transportné kódovania**

5.1. *Nespracované (Raw)*

Pri rozhraniach pre nešpecifikované (ľubovoľné) údaje možno prenášať kontajner HCERT a jeho nosný obsah tak, ako sú, s využitím akéhokoľvek základného transportu údajov, ktorý je bezpečný z hľadiska 8-bitového kódovania a spoľahlivý. Tieto rozhrania môžu zahŕňať komunikáciu na krátke vzdialenosti (NFC), Bluetooth alebo prenos prostredníctvom protokolu aplikačnej vrstvy, napríklad prenos potvrdenia HCERT od vystaviteľa do mobilného zariadenia držiteľa.

Ak sa pri prenose potvrdenia HCERT od vystaviteľa k držiteľovi používa rozhranie len s možnosťou zobrazenia (napríklad SMS, e-mail:), nespracované transportné kódovanie nie je zo zrejmých dôvodov použiteľné.

5.2. *Čiarový kód*

5.2.1. Kompresia nosného obsahu (CWT)

S cieľom zmenšiť veľkosť a zlepšiť rýchlosť a spoľahlivosť procesu načítania potvrdenia HCERT sa CWT komprimuje pomocou formátu ZLIB (RFC 1950 ([9])) a kompresného mechanizmu Deflate vo formáte vymedzenom v dokumente RFC 1951 ([10]).

5.2.2. Dvojrozmerný čiarový kód QR

Aby sa zabezpečila lepšia kompatibilita so staršími zariadeniami navrhnutými na spracúvanie nosného obsahu vo formáte ASCII, komprimovaný CWT sa kóduje vo formáte ASCII pomocou kódovania Base45 pred tým, ako sa zakóduje do dvojrozmerného čiarového kódu.

Na generovanie dvojrozmerného čiarového kódu sa použije formát QR vymedzený v norme (ISO/IEC 18004:2015). Odporúča sa miera korekcie chýb „Q“ (približne 25 %). Keďže sa Base45, QR kód musí používať alfanumerické kódovanie (režim 2 označený symbolmi 0010).

Aby mohli overovatelia zistiť typ zakódovaných údajov a vybrať správnu schému na dekódovanie a spracovanie, pred údajmi s kódovaním Base45 (podľa tejto špecifikácie) sa uvedie reťazec identifikátora kontextu „HC1:“. V budúcich verziách tejto špecifikácie, ktoré budú mať vplyv na spätnú kompatibilitu, sa vymedzí nový identifikátor kontextu, pričom znak nasledujúci za reťazcom „HC“ sa zvolí zo súboru znakov [1-9A-Z]. Poradie prírastkov sa vymedzuje tak, aby zodpovedalo tomuto poradiu, t. j. najskôr [1-9] a potom [A-Z].

Odporúča sa, aby bol optický kód na prezentačnom médiu vykreslený s uhlopriečkou od 35 mm do 60 mm, čo vyhovuje čítacím zariadeniam s pevnou optikou, pri ktorých je potrebné umiestniť prezentačné médium na povrch čítacieho zariadenia.

Ak sa optický kód tlačí na papier pomocou tlačiarní s nízkym rozlíšením (< 300 dpi), je nevyhnutné zabezpečiť, aby mal každý symbol (bod) kódu QR presne štvorcový tvar. V prípade neproporcionálnej zmeny mierky budú v niektorých riadkoch alebo stĺpcoch kódu QR symboly s obdĺžnikovým tvarom, čím sa v mnohých prípadoch sťaží čitateľnosť.

6. **Formát dôveryhodných zoznamov (zoznam CSCA a DSC)**

Od každého členského štátu sa vyžaduje poskytnutie zoznamu jedného alebo viacerých národných orgánov certifikácie podpisov (CSCA) a zoznamu všetkých platných certifikátov podpisovateľa dokumentov (DSC), ako aj udržiavanie týchto zoznamov v aktualizovanom stave.

6.1. *Zjednodušené riešenie z hľadiska orgánov CSCA/certifikátov DSC*

Pri tejto verzii špecifikácií členské štáty nepredpokladajú, že sa budú používať akékoľvek informácie o zozname zrušených certifikátov, ani že budú implementátori overovať obdobie používania súkromného kľúča.

Namiesto toho je hlavným mechanizmom na overenie platnosti to, že sa certifikát uvádza v najaktuálnejšej verzii daného zoznamu certifikátov.

([9]) rfc1950 (ietf.org).
([10]) rfc1951 (ietf.org).

6.2. *Infraštruktúra verejných kľúčov ICAO eMRTD a centrá dôveryhodnosti*

Členské štáty môžu použiť samostatný orgán CSCA, môžu však predložiť aj svoje existujúce certifikáty eMRTD CSCA a/alebo DSC, prípadne sa môžu rozhodnúť, že si ich obstarajú z (komerčných) centier dôveryhodnosti a predložia tie. Každý certifikát DSC však musí byť vždy podpísaný orgánom CSCA, ktorý daný členský štát oznámil.

7. **Bezpečnostné aspekty**

Pri návrhu schémy s využitím tejto špecifikácie musia členské štáty identifikovať, analyzovať a monitorovať určité bezpečnostné aspekty.

Do úvahy by sa mali vziať prinajmenšom tieto aspekty:

7.1. *Čas platnosti podpisu potvrdenia HCERT*

Vystaviteľ potvrdení HCERT je povinný obmedziť obdobie platnosti podpisu určením času uplynutia platnosti podpisu. Tým sa od držiteľa zdravotného potvrdenia vyžaduje, aby si ho v pravidelných intervaloch obnovoval.

Prijateľné obdobie platnosti môže byť určené na základe praktických obmedzení. Napríklad cestujúci nemusí mať možnosť obnoviť si zdravotné potvrdenie počas cesty do zahraničia. Môže však ísť aj o prípad, že vystaviteľ uvažuje nad možnosťou určitého narušenia zabezpečenia, keď by musel vystaviteľ odvolať certifikát DSC (čím by sa zneplatnili všetky zdravotné potvrdenia vystavené pomocou príslušného kľúča, pri ktorom ešte neuplynulo obdobie platnosti). Dôsledky takejto udalosti možno obmedziť pravidelným nasadzovaním kľúčov vystaviteľa a požadovaním obnovenia všetkých zdravotných potvrdení v určitom primeranom intervale.

7.2. *Správa kľúčov*

Táto špecifikácia vychádza vo veľkej miere zo silných kryptografických mechanizmov s cieľom zabezpečiť integritu údajov a overenie pôvodu údajov. Je preto nevyhnutné zachovanie dôvernosti súkromných kľúčov.

K narušeniu dôvernosti kryptografických kľúčov môže dôjsť rôznymi spôsobmi, napríklad:

— proces generovania kľúčov môže byť chybný, takže vygenerované kľúče sú slabé,

— kľúče môžu byť odhalené v dôsledku ľudskej chyby,

— môže dôjsť ku krádeži kľúčov páchateľmi z vonkajšieho alebo vnútorného prostredia,

— kľúče môžu byť vypočítané pomocou kryptoanalýzy.

S cieľom zmierniť riziká, že podpisový algoritmus sa ukáže ako slabý, čím sa umožní narušenie súkromných kľúčov pomocou kryptoanalýzy, sa v tejto špecifikácii odporúča, aby všetci účastníci zaviedli sekundárny záložný podpisový algoritmus, ktorý vychádza z odlišných parametrov alebo odlišného matematického problému než primárny algoritmus.

Pokiaľ ide o uvedené riziká v súvislosti s prevádzkovými prostrediami vystaviteľov, musia sa zaviesť zmierňujúce opatrenia na zabezpečenie účinnej kontroly, napríklad generovanie, ukladanie a používanie súkromných kľúčov v hardvérových bezpečnostných moduloch. Dôrazne sa odporúča používanie hardvérových bezpečnostných modulov na podpisovanie zdravotných potvrdení.

Bez ohľadu na to, či sa vystaviteľ rozhodne používať hardvérové bezpečnostné moduly, mal by sa stanoviť plán aktualizácií kľúčov, v ktorom by frekvencia aktualizácií kľúčov bola úmerná vystaveniu kľúčov externým sieťam, iným systémom a pracovníkom. Vhodne zvoleným plánom aktualizácií sa obmedzujú aj riziká súvisiace s chybne vystavenými zdravotnými potvrdeniami, keďže vystaviteľ má v prípade potreby možnosť zrušiť takéto zdravotné potvrdenia v dávkach odvolaním kľúča.

7.3. *Validácia vstupných údajov*

Tieto špecifikácie možno použiť spôsobom, pri ktorom sa predpokladá prijímanie údajov z nedôveryhodných zdrojov do systémov, ktoré môžu mať kritický význam. Aby sa minimalizovali riziká súvisiace s týmto vektorom útoku, všetky vstupné polia musia byť riadne validované podľa typov, dĺžok a obsahu údajov. Aj podpis vystaviteľa sa musí overiť, skôr ako dôjde k akémukoľvek spracovaniu obsahu potvrdenia HCERT. Pri overení podpisu vystaviteľa sa však predpokladá, že sa najskôr analyzuje chránené záhlavie vystaviteľa, v ktorom sa potenciálny útočník môže pokúsiť vsunúť starostlivo pripravené informácie navrhnuté s cieľom narušiť zabezpečenie systému.

8. **Správa dôveryhodnosti**

Na overenie podpisu potvrdenia HCERT sa vyžaduje verejný kľúč. Členské štáty sprístupnia tieto verejné kľúče. V konečnom dôsledku musí mať každý overovateľ zoznam všetkých verejných kľúčov, ktorým je ochotný dôverovať (keďže verejný kľúč nie je súčasťou potvrdenia HCERT).

Systém je zložený (len) z dvoch vrstiev: v každom členskom štáte je to jeden alebo viacero certifikátov na úrovni krajiny, ktoré slúžia na podpisovanie jedného alebo viacerých certifikátov podpisovateľa dokumentov (DSC), ktoré sa používajú v každodennej prevádzke.

Certifikáty členských štátov sa označujú ako certifikáty národných orgánov certifikácie podpisov (CSCA) a sú (zvyčajne) samopodpísané. Členské štáty môžu mať viacero takýchto certifikátov (napríklad v prípade regionálneho prenesenia právomocí). Tieto certifikáty CSCA slúžia na pravidelné podpisovanie certifikátov podpisovateľa dokumentov (DSC), pomocou ktorých sa podpisujú potvrdenia HCERT.

„Sekretariát" predstavuje funkčnú rolu. Pravidelne zhromažďuje a zverejňuje certifikáty DSC členských štátov po ich overení na základe zoznamu certifikátov CSCA (ktoré sa preniesli a overili inými prostriedkami).

Vo výslednom zozname certifikátov DSC sa potom bude nachádzať súhrnný súbor akceptovateľných verejných kľúčov (a zodpovedajúcich identifikátorov kľúčov – kid), pomocou ktorých môžu overovatelia validovať podpisy v potvrdeniach HCERT. Overovatelia musia pravidelne získavať a aktualizovať tento zoznam.

Formát takýchto osobitných zoznamov členských štátov sa môže prispôsobiť ich vlastným vnútroštátnym podmienkam. Formát súboru tohto dôveryhodného zoznamu sa ako taký môže líšiť, môže to byť napríklad podpísaný JWKS (formát súboru JWK podľa časti 5 dokumentu RFC 7517 ([11])) alebo akýkoľvek iný formát špecificky zodpovedajúci technológii používanej v danom členskom štáte.

V záujme jednoduchosti môžu členské štáty buď predložiť svoje existujúce certifikáty CSCA zo svojich systémov ICAO eMRTD, alebo podľa odporúčaní WHO vytvoriť takýto certifikát osobitne pre túto zdravotnú oblasť.

8.1. *Identifikátor kľúča (kid)*

Identifikátor kľúča (kid) sa vypočíta pri vytváraní zoznamu dôveryhodných verejných kľúčov z certifikátov DSC a skladá sa zo skráteného (prvých 8 bajtov) odtlačku SHA-256 certifikátu DSC zakódovaného v (nespracovanom) formáte DER.

Overovatelia nemusia vypočítať identifikátor kid na základe certifikátu DSC a môžu priamo priradiť identifikátor kľúča vo vydanom zdravotnom potvrdení k identifikátoru kid v dôveryhodnom zozname.

8.2. *Rozdiely voči modelu zabezpečenia dôveryhodnosti infraštruktúry verejných kľúčov ICAO eMRTD*

Hoci sa vychádza z najlepších postupov modelu zabezpečenia dôveryhodnosti infraštruktúry verejných kľúčov ICAO eMRTD, v záujme rýchlosti sa pristúpilo k viacerým zjednodušeniam:

— Členské štáty môžu predložiť viaceré certifikáty CSCA.

— Môže sa nastaviť akákoľvek dĺžka obdobia platnosti certifikátu DSC (používanie kľúča), ktorá neprekračuje obdobie platnosti certifikátu CSCA, a obdobie platnosti nemusí byť uvedené.

— Certifikát DSC môže obsahovať identifikátory politiky (rozšírené používanie kľúča), ktoré sú špecifické pre zdravotné potvrdenia.

— Členské štáty sa môžu rozhodnúť, že nebudú nikdy vykonávať overenie zverejnených zrušení, ale že sa namiesto toho budú spoliehať len na zoznamy certifikátov DSC, ktoré na dennej báze prijímajú od sekretariátu, alebo si budú zostavovať vlastné zoznamy.

([11]) rfc7517 (ietf.org).

PRÍLOHA II

PRAVIDLÁ NA ÚČELY VYPĹŇANIA DIGITÁLNEHO COVID PREUKAZU EÚ

Cieľom všeobecných pravidiel týkajúcich sa súborov hodnôt, ktoré sa stanovujú v tejto prílohe, je zabezpečiť interoperabilitu na sémantickej úrovni a umožniť jednotné technické vykonávanie pre digitálny COVID preukaz EÚ. Prvky uvedené v tejto prílohe možno použiť v troch odlišných kontextoch (očkovanie/testovanie/prekonanie ochorenia), ako sa uvádza v nariadení (EÚ) 2021/953. V tejto prílohe sa uvádzajú len prvky, pri ktorých sa vyžaduje sémantická normalizácia prostredníctvom kódovaných súborov hodnôt.

Za preklad kódovaných prvkov do svojho úradného jazyka zodpovedajú príslušné členské štáty.

Pre všetky dátové polia, ktoré nie sú uvedené v nasledujúcich opisoch súborov hodnôt, sa odporúča kódovanie UTF-8 (meno, testovacie centrum, vystaviteľ potvrdenia). V prípade dátových polí obsahujúcich kalendárne dátumy (dátum narodenia, dátum očkovania, dátum a čas odberu testovanej vzorky, dátum prvého pozitívneho výsledku testu, dátumy platnosti potvrdenia) sa odporúča kódovanie podľa normy ISO 8601.

Ak z akéhokoľvek dôvodu nemožno použiť uprednostňované systémy kódov uvedené ďalej, môžu sa použiť iné medzinárodné systémy kódov a malo by sa zverejniť usmernenie k spôsobu priradenia kódov z iného systému kódov k uprednostňovanému systému kódov. Vo výnimočných prípadoch sa môže použiť text (zobrazované názvy) ako záložný mechanizmus, keď vo vymedzených súboroch hodnôt nie je k dispozícii vhodný kód.

Členské štáty, ktoré vo svojich systémoch používajú iné kódovanie, by mali priradiť takéto kódy k opísaným súborom hodnôt. Za každé takéto priradenie zodpovedajú členské štáty.

Komisia s podporou siete elektronického zdravotníctva a Výboru pre zdravotnú bezpečnosť súbory hodnôt pravidelne aktualizuje. Aktualizované súbory hodnôt sa zverejnia na príslušných webových stránkach Komisie, ako aj na webovej stránke siete elektronického zdravotníctva. Je potrebné sprístupniť históriu zmien.

1. **Ochorenie alebo pôvodca ochorenia, na ktoré sa potvrdenie vzťahuje/ochorenie alebo pôvodca ochorenia, ktoré držiteľ prekonal: ochorenie COVID-19 (vírus SARS-CoV-2 alebo niektorý z jeho variantov)**

   Uprednostňovaný systém kódov: SNOMED CT.

   Má sa používať v potvrdení 1, 2 a 3.

   Zvolené kódy označujú ochorenie COVID-19 alebo, ak sa vyžadujú podrobnejšie informácie o genetickom variante vírusu SARS-CoV-2, tieto varianty, ak sa z epidemiologických dôvodov vyžadujú takéto podrobné informácie.

   Príkladom kódu, ktorý by sa mal použiť, je kód SNOMED CT 840539006 (COVID-19).

2. **Vakcína alebo profylaxia proti ochoreniu COVID-19**

   Uprednostňovaný systém kódov: SNOMED CT alebo klasifikácia ATC.

   Má sa používať v potvrdení 1.

   Medzi príklady kódov, ktoré by sa mali použiť z uprednostňovaných systémov kódov, patrí kód SNOMED CT 1119305005 (vakcína s antigénmi proti vírusu SARS-CoV-2), 1119349007 (vakcína mRNA proti vírusu SARS-CoV-2) alebo J07BX03 (vakcíny proti ochoreniu COVID-19). Súbor hodnôt by sa mal rozšíriť, keď sa vyvinú a začnú používať nové typy vakcín.

3. **Vakcinačná látka proti ochoreniu COVID-19**

   Uprednostňované systémy kódov (v uprednostňovanom poradí):

   — register liekov Únie pre vakcíny s povolením pre celú EÚ (čísla povolení),

   — celosvetový register vakcín, napríklad register, ktorý by mohla zriadiť Svetová zdravotnícka organizácia,

   — v ostatných prípadoch názov vakcinačnej látky. Ak názov obsahuje medzery, mali by sa nahradiť spojovníkom (-).

Názov súboru hodnôt: Vakcína.

Má sa používať v potvrdení 1.

Príkladom kódu, ktorý by sa mal použiť z uprednostňovaných systémov kódov, je EU/1/20/1528 (Comirnaty). Príklad názvu vakcíny, ktorý sa má použiť ako kód: Sputnik-V (označuje Sputnik V).

4. **Držiteľ povolenia na uvedenie na trh vakcíny proti ochoreniu COVID-19 alebo jej výrobca**

Uprednostňovaný systém kódov:

— kód organizácie podľa EMA (systém SPOR pre normu ISO IDMP),

— celosvetový register držiteľov povolenia na uvedenie na trh alebo výrobcov vakcín, napríklad register, ktorý by mohla zriadiť Svetová zdravotnícka organizácia,

— v ostatných prípadoch názov organizácie. Ak názov obsahuje medzery, mali by sa nahradiť spojovníkom (-).

Má sa používať v potvrdení 1.

Príkladom kódu, ktorý by sa mal použiť z uprednostňovaného systému kódov, je ORG-100001699 (AstraZeneca AB). Príklad názvu organizácie, ktorý sa má použiť ako kód: Sinovac-Biotech (označuje Sinovac Biotech).

5. **Poradie v sérii dávok, ako aj celkový počet dávok v sérii**

Má sa používať v potvrdení 1.

Dve polia:

1. počet dávok podaných v rámci cyklu;

2. počet očakávaných dávok pre ukončený cyklus (špecifický pre osobu v čase podania).

Napríklad hodnoty 1/1, 2/2 budú vyjadrovať ukončený cyklus, a to vrátane možnosti 1/1 pre vakcíny s dvomi dávkami, v prípade ktorých sa však na základe protokolu uplatňovaného v členskom štáte podáva jedna dávka občanom, ktorým sa pred očkovaním diagnostikovalo ochorenie COVID-19. Celkový počet dávok v sérii by sa mal uvádzať na základe informácií dostupných v čase podania dávky. Ak sa napríklad pri určitej vakcíne vyžaduje tretia (posilňovacia) dávka v čase poslednej podanej dávky, má sa to zohľadniť v druhom čísle v poli (napríklad 2/3, 3/3 atď.).

6. **Členský štát alebo tretia krajina, kde bola podaná vakcína/kde sa vykonal test**

Uprednostňovaný systém kódov: kódy krajiny podľa normy ISO 3166.

Má sa používať v potvrdení 1, 2 a 3.

Obsah súboru hodnôt: úplný zoznam kódov pozostávajúcich z dvoch písmen, k dispozícii ako súbor hodnôt vymedzených v rámci FHIR (http://hl7.org/fhir/ValueSet/iso3166-1-2).

7. **Typ testu**

Uprednostňovaný systém kódov: LOINC.

Má sa používať v potvrdení 2 a v potvrdení 3, ak sa prostredníctvom delegovaného aktu zavedie podpora pre vydávanie potvrdení o prekonaní ochorenia na základe iných typov testov, než je test NAAT.

Kódy v tomto súbore hodnôt odkazujú na spôsob testu a vyberajú sa prinajmenšom na oddelenie testov NAAT od rýchlych antigénových testov, ako sú vyjadrené v nariadení (EÚ) 2021/953.

Príklad kódu, ktorý by sa mal použiť z uprednostňovaného systému kódov, je LP217198-3 (rýchly imunologický test).

8. **Výrobca a obchodný opis použitého testu (voliteľné pre test NAAT)**

Uprednostňovaný systém kódov: zoznam rýchlych antigénových testov Výboru pre zdravotnú bezpečnosť vedený Spoločným výskumným centrom (databáza diagnostických pomôcok a testovacích metód in vitro zameraných na COVID-19).

Má sa používať v potvrdení 2.

Obsah súboru hodnôt zahŕňa výber rýchlych antigénových testov, ako sa uvádzajú v spoločnom a aktualizovanom zozname rýchlych antigénových testov na COVID-19 vytvorenom na základe odporúčania Rady 2021/C 24/01, ktorý odsúhlasil Výbor pre zdravotnú bezpečnosť. Zoznam vedie Spoločné výskumné centrum v databáze diagnostických pomôcok a testovacích metód in vitro zameraných na COVID-19 na adrese: https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat.

V prípade tohto systému kódov sa použijú príslušné polia, ako je identifikátor testovacej pomôcky, názov testu a výrobca, a to podľa štruktúrovaného formátu Spoločného výskumného centra, ktorý je k dispozícii na adrese: https://covid-19-diagnostics.jrc.ec.europa.eu/devices.

9. **Výsledok testu**

Uprednostňovaný systém kódov: SNOMED CT.

Má sa používať v potvrdení 2.

Zvolené kódy umožnia odlíšiť pozitívne výsledky testu od negatívnych (zistené alebo nezistené). Dodatočné hodnoty (ako neurčené) sa môžu pridať, ak si to vyžadujú prípady použitia.

Príklady kódov, ktoré by sa mali použiť z uprednostňovaného systému kódov, sú 260415000 (nezistené) a 260373001 (zistené).

PRÍLOHA III:

SPOLOČNÁ ŠTRUKTÚRA JEDINEČNÉHO IDENTIFIKÁTORA POTVRDENIA

1. **Úvod**

Každý digitálny COVID preukaz EÚ obsahuje jedinečný identifikátor potvrdenia (ďalej len „UCI“), ktorý podporuje interoperabilitu digitálneho COVID preukazu EÚ. Jedinečný identifikátor potvrdenia sa môže použiť na overenie potvrdenia. Členské štáty sú zodpovedné za zavedenie jedinečného identifikátora potvrdenia. Jedinečný identifikátor potvrdenia je prostriedok na overenie pravosti potvrdenia, prípadne na prepojenie na registračný systém (napríklad IIS). Tieto identifikátory zároveň musia členským štátom umožňovať (v papierovej a digitálnej podobe) vyhlásiť, že jednotlivci boli očkovaní alebo testovaní.

2. **Zloženie jedinečného identifikátora potvrdenia**

Jedinečný identifikátor potvrdenia má spoločnú štruktúru a formát, ktoré uľahčujú ľudskú a/alebo strojovú čitateľnosť informácií a ktoré sa môžu týkať prvkov, ako je členský štát očkovania, samotná očkovacia látka a špecifický identifikátor členského štátu. Členským štátom poskytuje flexibilitu pri formátovaní, a to pri plnom rešpektovaní právnych predpisov v oblasti ochrany údajov. Z hľadiska poradia osobitných prvkov sa dodržiava vymedzená hierarchia, vďaka ktorej sú možné budúce úpravy blokov pri súčasnom zachovaní štrukturálnej integrity.

Možné riešenia zloženia UCI tvoria spektrum, v ktorom sa uplatňuje modularita a ľudská čitateľnosť ako dva hlavné diverzifikujúce parametre, ako aj jedna základná vlastnosť:

— modularita: miera, do akej je kód zložený zo samostatných stavebných blokov, ktoré obsahujú sémanticky odlišné informácie,

— ľudská čitateľnosť: miera, do akej je kód zmysluplný alebo čitateľný pre človeka,

— globálna jedinečnosť: identifikátor krajiny alebo orgánu je vhodne riadený a očakáva sa, že každá krajina (orgán) vhodne riadi svoj segment priestoru názvov tak, aby sa identifikátory nikdy nerecyklovali ani sa opätovne nevydávali. Touto kombináciou sa zabezpečí, že každý identifikátor je globálne jedinečný.

3. **Všeobecné požiadavky**

Vo vzťahu k UCI sa vyžaduje splnenie týchto súhrnných požiadaviek:

1. znaková sada: povoľujú sa len alfanumerické znaky veľkých písmen US-ASCII („A“ až „Z“, „0“ až „9“) s dodatočnými osobitnými oddeľovacími znakmi z dokumentu RFC 3986 ([1]) ([2]), konkrétne {„/“, „#“, „:“};

2. maximálna dĺžka: tvorcovia by sa mali snažiť dodržať dĺžku 27 – 30 znakov ([3]);

3. predpona verzie: vzťahuje sa na verziu schémy UCI. Predpona verzie je „01“ pre túto verziu dokumentu; predpona verzie je zložená z dvoch číslic;

4. predpona krajiny: kód krajiny sa určuje na základe normy ISO 3166-1. Dlhšie kódy (napr. 3 a viac znakov [napríklad „UNHCR“]) sú vyhradené na budúce použitie;

5. prípona kódu/kontrolný súčet:

5.1. Členské štáty by mali využiť kontrolný súčet, keď je pravdepodobné, že môže dôjsť k prenosu, prepisu (človekom) alebo k iným znehodnoteniam (napríklad pri použití v tlačenej podobe).

5.2. Na kontrolný súčet sa nemožno spoliehať pri overovaní platnosti potvrdenia a technicky nie je súčasťou identifikátora, ale slúži na overenie integrity kódu. Týmto kontrolným súčtom má byť zhrnutie celého UCI v digitálnom/elektronickom prenosovom formáte podľa normy ISO-7812-1 (LUHN-10) ([4]). Kontrolný súčet je od zvyšku UCI oddelený znakom „#“.

([1]) rfc3986 (ietf.org).

([2]) Polia ako pohlavie, identifikačné číslo šarže (dávky), očkovacie stredisko, identifikácia zdravotníckeho pracovníka, ďalší dátum očkovania nemusia byť potrebné na iné účely ako na lekárske použitie.

([3]) Na používanie QR kódov by členské štáty mohli zvážiť dodatočný súbor znakov do celkovej dĺžky 72 znakov (vrátane 27 – 30 znakov samotného identifikátora), ktorý sa môže použiť na poskytnutie ďalších informácií. Špecifikáciu týchto informácií vymedzia členské štáty.

([4]) Luhnov algoritmus modulo N je rozšírením Luhnovho algoritmu (známeho aj ako algoritmus modulo 10), ktorý funguje pre číselné kódy a používa sa napríklad na výpočet kontrolného súčtu kreditných kariet. Týmto rozšírením sa umožní, aby algoritmus fungoval so sekvenciami hodnôt na akomkoľvek základe (v našom prípade abecedné znaky).

Mala by sa zabezpečiť spätná kompatibilita: členské štáty, ktoré postupom času zmenia štruktúru svojich identifikátorov (v rámci hlavnej verzie, v súčasnosti stanovenej na v1), musia zabezpečiť, že akékoľvek dva identické identifikátory sa vzťahujú na rovnaké potvrdenie/vyhlásenie o očkovaní. Inými slovami, členské štáty nemôžu identifikátory recyklovať.

4. **Možnosti jedinečného identifikátora potvrdenia pre potvrdenia o očkovaní**

V usmerneniach siete elektronického zdravotníctva o overiteľných potvrdeniach o očkovaní a základných prvkoch interoperability ([5]) sa uvádzajú rôzne možnosti dostupné členským štátom a iným stranám, ktoré môžu súbežne existovať naprieč rôznymi členskými štátmi. Členské štáty môžu využiť takéto rôzne možnosti v rôznych verziách schémy UCI.

([5]) https://ec.europa.eu/health/sites/default/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf.

PRÍLOHA IV

SPRÁVA CERTIFIKÁTOV VEREJNÉHO KĽÚČA

1. Úvod

Bezpečná a dôveryhodná výmena podpisových kľúčov pre digitálne COVID preukazy EÚ (ďalej len „DCC“) medzi členskými štátmi sa realizuje prostredníctvom brány digitálnych COVID preukazov EÚ (ďalej len „DCCG“), ktorá slúži ako centrálne úložisko verejných kľúčov. Členské štáty sú prostredníctvom DCCG oprávnené zverejňovať verejné kľúče zodpovedajúce súkromným kľúčom, ktoré využívajú na podpisovanie digitálnych COVID preukazov. Členské štáty, ktoré túto možno využívajú, môžu použiť DCCG na včasné získanie aktuálneho materiálu verejných kľúčov. DCCG sa neskôr môže rozšíriť na výmenu dôveryhodných doplňujúcich informácií, ktoré poskytujú členské štáty, ako sú pravidlá validácie DCC. Modelom dôvery rámca DCC je infraštruktúra verejných kľúčov (PKI). Každý členský štát udržiava jeden alebo viac národných orgánov certifikácie podpisov (ďalej len „CSCA“), ktorých certifikáty majú pomerne dlhú životnosť. Na základe rozhodnutia členského štátu môže byť CSCA rovnaký alebo odlišný od CSCA použitého v prípade strojovo čitateľných cestovných dokladov. CSCA vystavuje certifikáty verejného kľúča pre vnútroštátnych, krátkodobých podpisovateľov dokumentov (t. j. podpisujúce subjekty pre DCC), ktoré sa označujú ako certifikáty podpisovateľa dokumentov (ďalej len „DSC“). CSCA vystupuje ako bod dôvery (trust anchor), aby členské štáty, ktoré túto možno využívajú, mohli využiť certifikát CSCA na overenie pravosti a integrity pravidelne sa meniacich certifikátov DSC. Po validácii môžu členské štáty poskytnúť tieto certifikáty (alebo len v nich obsiahnuté verejné kľúče) svojim aplikáciám na validáciu DCC. DCCG sa okrem CSCA a DSC spolieha aj na PKI pri autentifikácii transakcií a podpisovaní údajov, pričom slúži aj ako základ pre autentifikáciu a ako prostriedok na zabezpečenie integrity komunikačných kanálov medzi členskými štátmi a DCCG.

Na zaistenie integrity a pravosti údajov je možné použiť digitálne podpisy. Infraštruktúry verejných kľúčov vytvárajú dôveru previazaním verejných kľúčov s overenými identitami (alebo vystaviteľmi). To je nevyhnutné, aby si ostatní účastníci mohli overiť pôvod údajov a identitu komunikačného partnera a rozhodnúť sa, či im budú dôverovať. V DCGG sa v záujme zabezpečenia pravosti využívajú viaceré certifikáty verejného kľúča. V tejto prílohe sa vymedzuje, ktoré certifikáty verejného kľúča sa využívajú a ako by sa mali navrhnúť, aby umožnili širokú interoperabilitu medzi členskými štátmi. Poskytujú sa v nej ďalšie podrobnosti o potrebných certifikátoch verejného kľúča a uvádza sa v nej usmernenie o vzoroch certifikátov a obdobiach platnosti pre členské štáty, ktoré chcú prevádzkovať svoje vlastné CSCA. Keďže DCC musia byť overiteľné počas vymedzeného časového rámca (počnúc vydaním, pričom platnosť uplynie po danom čase), je potrebné vymedziť model overenia pre všetky podpisy použité na certifikátoch verejného kľúča a DCC.

2. Terminológia

V nasledujúcej tabuľke sa uvádzajú skratky a terminológia použitá v tejto prílohe.

Termín	Vymedzenie pojmu
Certifikát	Alebo certifikát verejného kľúča. Certifikát X.509 v3, ktorý obsahuje verejný kľúč subjektu
CSCA	Národný orgán certifikácie podpisov
DCC	Digitálny COVID preukaz EÚ. Podpísaný digitálny dokument, ktorý obsahuje informácie o očkovaní, testovaní alebo prekonaní ochorenia
DCCG	Brána digitálneho COVID preukazu EÚ. Tento systém sa používa na výmenu DSC medzi členskými štátmi.
$DCCG_{TA}$	Certifikát bodu dôvery DCCG. Zodpovedajúci súkromný kľúč sa používa na podpísanie zoznamu všetkých certifikátov CSCA offline
$DCCG_{TLS}$	Certifikát TLS servera DCCG
DSC	Certifikát podpisovateľa dokumentov. Certifikát verejného kľúča orgánu členského štátu podpisujúceho dokumenty (napríklad systém, ktorý má povolenie podpisovať DCC). Tento certifikát vystavuje CSCA členského štátu.
EC-DSA	Algoritmus digitálneho podpisu na báze eliptických kriviek (Elliptic Curve Digital Signature Algorithm). Algoritmus kryptografického podpisu na základe eliptických kriviek
Členský štát	členský štát Európskej únie

Termín	Vymedzenie pojmu
mTLS	Vzájomný protokol TLS Protokol TLS (Transport Layer Security) so vzájomnou autentifikáciou
NB	Vnútroštátny spracovateľský subjekt („backend“) členského štátu
NB_{CSCA}	Certifikát národného orgánu certifikácie podpisov členského štátu (môže ich byť viacero)
NB_{TLS}	Certifikát klientskej autentifikácie TLS vnútroštátneho spracovateľského subjektu
NB_{UP}	Certifikát, ktorý vnútroštátny spracovateľský subjekt používa na podpisovanie dátových balíkov, ktoré sa nahrávajú do DCCG
PKI	Infraštruktúra verejných kľúčov. Model dôvery založený na certifikátoch verejného kľúča a certifikačných autoritách
RSA	Asymetrický kryptografický algoritmus založený na celočíselnej faktorizácii, ktorý sa používa pre digitálne podpisy alebo asymetrické šifrovanie

3. **Komunikačné toky a služby zabezpečenia DCCG**

V tomto oddiele sa uvádza prehľad komunikačných tokov a služieb zabezpečenia v systéme DCCG. Takisto sa v ňom vymedzuje, ktoré kľúče a certifikáty sa používajú na ochranu komunikácie, nahraných informácií, DCC a podpísaného dôveryhodného zoznamu, ktorý obsahuje všetky nahrané certifikáty CSCA. Brána DCCG funguje ako dátový uzol, ktorý umožňuje výmenu podpísaných balíkov údajov pre členské štáty.

Nahrané balíky údajov poskytuje DCCG „tak, ako sú“, čo znamená, že DCCG nepridáva ani neodstraňuje DSC v prípade balíkov, ktoré prijíma. Vnútroštátny spracovateľský subjekt (national backend – NB) členských štátov musí byť schopný overiť integritu a pravosť nahraných údajov medzi koncovými bodmi. Vnútroštátne spracovateľské subjekty a DCCG okrem toho využijú vzájomnú autentifikáciu TLS na vytvorenie zabezpečeného spojenia. Predstavuje to dodatok k podpisom vo vymieňaných údajoch.

3.1. *Autentifikácia a nadviazanie spojenia*

DCCG používa zabezpečenie TSL (Transport Layer Security) so vzájomnou autentifikáciou s cieľom vytvoriť autentifikovaný šifrovaný kanál medzi vnútroštátnym spracovateľským subjektom (NB) členského štátu a prostredím brány. DCCG má preto serverový certifikát TLS (skratka $DCCG_{TLS}$) a vnútroštátny spracovateľský subjekt má klientský certifikát TLS (skratka NB_{TLS}). Vzory certifikátov sa uvádzajú v *oddiele 5*. Každý vnútroštátny spracovateľský subjekt môže poskytnúť svoj vlastný certifikát TLS. Tento certifikát sa výslovne uvedie na bielu listinu, a teda ho môže vystaviť verejne dôveryhodná certifikačná autorita (napríklad certifikačná autorita, ktorá dodržiava základné požiadavky organizácie CA/Browser Forum), národná certifikačná autorita alebo môže ísť o samopodpísaný certifikát. Každý členský štát je zodpovedný za svoje vnútroštátne údaje a za ochranu súkromného kľúča použitého na vytvorenie spojenia s DCCG. Prístup na základe poskytnutia vlastného certifikátu si vyžaduje vhodne vymedzený proces registrácie a identifikácie, ako aj postupy zrušenia a obnovenia, ako sa uvádza v *oddieloch 4.1, 4.2* a *4.3*. DSSG využíva bielu listinu, na ktorú sa po úspešnej registrácii pridávajú certifikáty TLS vnútroštátnych spracovateľských subjektov. Len vnútroštátne spracovateľské subjekty, ktoré sa autentifikujú súkromným kľúčom, ktorý zodpovedá certifikátu z bielej listiny, môžu vytvoriť zabezpečené spojenie s DCCG. DCCG takisto použije certifikát TLS, ktorý vnútroštátnym spracovateľským subjektom umožňuje overiť, že naozaj vytvárajú spojenie so „skutočnou“ DCCG a nie so subjektom so zlými úmyslami, ktorý vystupuje ako DCCG. Certifikát DCCG sa poskytne vnútroštátnym spracovateľským subjektom po úspešnej registrácii. Certifikát $DCCG_{TLS}$ vystaví verejne dôveryhodná certifikačná autorita (začlenená vo všetkých hlavných prehliadačoch). Povinnosťou členských štátov je overiť, že je ich spojenie s DCCG zabezpečené (napríklad kontrolou odtlačku certifikátu $DCCG_{TLS}$ pripojeného servera voči odtlačku poskytnutému po registrácii).

3.2. *Národné orgány certifikácie podpisov a model validácie*

Členské štáty, ktoré sa zúčastňujú na rámci DCCG, musia pri vystavovaní DSC využiť CSCA. Členské štáty môžu mať viac než jeden CSCA, napríklad v prípade regionálneho prenesenia právomocí. Každý členský štát môže buď využiť existujúce certifikačné autority, alebo si pre systém DCC môže vytvoriť špecifickú certifikačnú autoritu (prípadne samopodpísanú).

Členské štáty musia predložiť svoj certifikát (certifikáty) CSCA prevádzkovateľovi DCCG počas oficiálneho postupu nadviazania spolupráce. Prevádzkovateľ DCCG po úspešnej registrácii členského štátu (*pozri ďalšie informácie v oddiele 4.1*) aktualizuje podpísaný dôveryhodný zoznam, ktorý obsahuje všetky certifikáty CSCA, ktoré sú aktívne v rámci DCC. Prevádzkovateľ DCCG použije vyhradený asymetrický kľúčový pár na podpísanie dôveryhodného zoznamu a certifikátov v offline prostredí. Súkromný kľúč sa nebude uchovávať v online systéme DCCG, aby narušenie online systému neumožnilo útočníkovi narušiť dôveryhodný zoznam. Zodpovedajúci certifikát bodu dôvery $DCCG_{TA}$ sa poskytne vnútroštátnym spracovateľským subjektom počas postupu nadviazania spolupráce.

Členské štáty môžu získať dôveryhodný zoznam od DCCG pre svoje postupy overenia. CSCA sa vymedzuje ako certifikačná autorita, ktorá vystavuje DSC, a teda členské štáty, ktoré využívajú viacúrovňovú hierarchiu certifikačných autorít (napríklad koreňová CA-> CSCA -> DSC), musia zabezpečiť podriadenú certifikačnú autoritu, ktorá vystavuje DSC. V tomto prípade, ak členský štát využíva existujúcu certifikačnú autoritu, systém DCC bude ignorovať všetko nad úrovňou CSCA a na bielu listinu uvedie len CSCA ako bod dôvery (hoci ide o podriadenú certifikačnú autoritu). Zodpovedá to modelu ICAO, umožňuje však len presne dve úrovne – „koreňový“ CSCA a koncový („listový“) DSC podpísaný len týmto CSCA.

Ak členský štát prevádzkuje vlastný CSCA, je daný členský štát zodpovedný za bezpečnú prevádzku a riadenie jeho kľúčov. CSCA pôsobí ako bod dôvery pre DSC, a preto je ochrana súkromného kľúča CSCA nevyhnutná pre integritu prostredia DCC. Model overovania v infraštruktúre verejných kľúčov DCC je tzv. shell model, podľa ktorého všetky certifikáty pri validácii cesty certifikátov musia byť platné v danom čase (t. j. v čase validácie podpisu). Uplatňujú sa preto tieto obmedzenia:

— CSCA nesmie vystavovať certifikáty, ktoré platia dlhšie ako samotný certifikát certifikačnej autority,

— podpisovateľ dokumentov nepodpíše dokumenty, ktoré platia dlhšie ako samotný DSC,

— členské štáty, ktoré prevádzkujú vlastný CSCA, musia vymedziť obdobia platnosti svojich CSCA a všetkých vystavených certifikátov a musia sa postarať o obnovovanie certifikátov.

V *oddiele 4.2* sa uvádzajú odporúčania pre obdobia platnosti.

3.3. *Integrita a pravosť nahraných údajov*

Vnútroštátne spracovateľské subjekty môžu použiť DCCG na nahranie a stiahnutie digitálne podpísaných balíkov údajov po úspešnej vzájomnej autentifikácii. Tieto balíky údajov na začiatku obsahujú DSC členských štátov. Kľúčový pár, ktorý používa vnútroštátny spracovateľský subjekt pre digitálny podpis nahraných balíkov údajov v systéme DCCG, sa nazýva kľúčový pár podpisu vnútroštátneho spracovateľského subjektu na nahrávanie a zodpovedajúci certifikát verejného kľúča sa skracuje ako certifikát NB_{UP}. Každý členský štát poskytne svoj vlastný certifikát NB_{UP}, ktorý môže byť samopodpísaný alebo ho môže vystaviť existujúca certifikačná autorita, ako je verejná certifikačná autorita (t. j. certifikačná autorita, ktorá vystavuje certifikáty v súlade so základnými požiadavkami organizácie CA/Browser Forum). Certifikát NB_{UP} musí byť odlišný od všetkých ostatných certifikátov využívaných členským štátom (t. j. CSCA, klientský TLS alebo DSC).

Členské štáty musia poskytnúť certifikát na nahrávanie prevádzkovateľovi DCCG pri prvej registrácii (*pozri ďalšie informácie v oddiele 4.1*). Každý členský štát je zodpovedný za svoje vnútroštátne údaje a musí chrániť súkromný kľúč, ktorý sa používa na podpísanie nahraných súborov.

Ostatné členské štáty môžu overiť podpísané balíky údajov pomocou certifikátov na nahrávanie, ktoré poskytuje DCCG. DCCG overuje pravosť a integritu nahraných údajov pomocou certifikátu vnútroštátneho spracovateľského subjektu na nahrávanie pred tým, ako sa poskytnú iným členským štátom.

3.4. *Požiadavky na technickú architektúru DCCG*

Pokiaľ ide o technickú architektúru DCCG, uplatňujú sa tieto požiadavky:

— DCCG využíva vzájomnú autentifikáciu TLS s cieľom nadviazať autentifikované šifrované spojenie s vnútroštátnymi spracovateľskými subjektmi. DCCG preto vedie bielu listinu registrovaných klientskych certifikátov NB_{TLS},

— DCCG používa dva digitálne certifikáty ($DCCG_{TLS}$ a $DCCG_{TA}$) s dvoma samostatnými kľúčovými pármi. Súkromný kľúč kľúčového páru $DCCG_{TA}$ sa uchováva offline (nie v online zložkách DCCG),

— DCCG vedie dôveryhodný zoznam certifikátov NB_{CSCA}, ktorý sa podpisuje súkromným kľúčom $DCCG_{TA}$,

— použité šifry musia spĺňať požiadavky uvedené v *oddiele 5.1*.

4. Riadenie životného cyklu certifikátov

4.1. *Registrácia vnútroštátnych spracovateľských subjektov*

Členské štáty sa musia zaregistrovať u prevádzkovateľa DCCG, aby sa mohli zapojiť do systému DCCG. V tomto oddiele sa opisuje technický a prevádzkový postup, ktorý sa musí dodržať pri registrácii vnútroštátneho spracovateľského subjektu.

Prevádzkovateľ DCCG a členský štát si musia vymieňať informácie o technických kontaktných osobách pre postup nadviazania spolupráce. Predpokladá sa, že technické kontaktné osoby sú legitimizované svojimi členskými štátmi a identifikácia/autentifikácia sa vykonáva prostredníctvom iných kanálov. Autentifikáciu je napríklad možné dosiahnuť, keď technická kontaktná osoba členského štátu poskytne certifikáty e-mailom ako súbory šifrované heslom a zodpovedajúce heslo oznámi prevádzkovateľovi DCCG telefonicky. Môžu sa využiť aj iné zabezpečené kanály vymedzené prevádzkovateľom DCCG.

Členský štát musí počas procesu registrácie a identifikácie poskytnúť tri digitálne certifikáty:

— certifikát TLS členského štátu – NB_{TLS},

— certifikát členského štátu na nahrávanie – NB_{UP},

— certifikát (certifikáty) CSCA členského štátu – NB_{CSCA}.

Všetky poskytnuté certifikáty musia spĺňať požiadavky vymedzené v *oddiele 5*. Prevádzkovateľ DCCG overí, či poskytnutý certifikát spĺňa požiadavky uvedené v *oddiele 5*. Prevádzkovateľ DCCG po identifikácii a registrácii:

— pridá certifikát (certifikáty) NB_{CSCA} do dôveryhodného zoznamu podpísaného súkromným kľúčom, ktorý zodpovedá verejnému kľúču $DCCG_{TA}$,

— pridá certifikát NB_{TLS} na bielu listinu koncového bodu TLS DCCG,

— pridá certifikát NB_{UP} do systému DCCG,

— poskytne certifikát verejného kľúča $DCCG_{TA}$ a $DCCG_{TLS}$ členskému štátu.

4.2. *Certifikačné autority, obdobia platnosti a obnovenie*

Ak chce členský štát prevádzkovať svoj vlastný CSCA, certifikáty CSCA môžu byť samopodpísané certifikáty. Vystupujú ako bod dôvery členského štátu, a preto musí členský štát dôsledne chrániť súkromný kľúč zodpovedajúci verejnému kľúču certifikátu CSCA. Odporúča sa, aby členské štáty pre svoje CSCA využívali offline systém, t. j. počítačový systém, ktorý nie je napojený k žiadnej sieti. Na prístup do systému sa využije kontrola viacerými osobami (napríklad podľa zásady štyroch očí). Po podpísaní DSC sa uplatnia operačné kontroly a systém, ktorý drží súkromný kľúč CSCA, sa bezpečne uloží s využitím silných prvkov kontroly prístupu. Na dodatočnú ochranu súkromného kľúča CSCA sa môžu využiť hardvérové bezpečnostné moduly alebo čipové karty. Digitálne certifikáty obsahujú obdobie platnosti, na základe ktorého sa vyžaduje obnovenie certifikátu. Obnovenie je nevyhnutné na použitie čerstvých kryptografických kľúčov a na prispôsobenie veľkostí kľúčov, keď nové vylepšenia z hľadiska výpočtov alebo nové útoky ohrozujú bezpečnosť použitého kryptografického algoritmu. Uplatňuje sa tzv. shell model (pozri *oddiel 3.2*).

Vzhľadom na ročnú platnosť digitálnych COVID preukazov EÚ sa odporúčajú tieto obdobia platnosti:

— CSCA: 4 roky

— DSC: 2 roky

— Nahrávanie: 1 až 2 roky

— Klientská autentifikácia TLS: 1 až 2 roky

Na včasnú obnovu sa odporúčajú tieto obdobia používania súkromných kľúčov:

— CSCA: 1 rok

— DSC: 6 mesiacov

Členské štáty musia včas vytvoriť nové certifikáty na nahrávanie a certifikáty TLS, napríklad jeden mesiac pred exspiráciou, aby sa zabezpečila plynulá prevádzka. Certifikáty CSCA a DSC by sa mali obnovovať aspoň mesiac pred skončením obdobia používania súkromného kľúča (vzhľadom na potrebné prevádzkové postupy). Členské štáty musia prevádzkovateľovi DCCG poskytnúť aktualizované certifikáty CSCA, certifikáty na nahrávanie a certifikáty TLS. Exspirované certifikáty sa odstránia z bielej listiny a z dôveryhodného zoznamu.

Členské štáty a prevádzkovateľ DCCG musia sledovať platnosť svojich certifikátov. Neexistuje žiadny centrálny subjekt, ktorý by zaznamenával platnosť certifikátov a informoval o nej účastníkov.

4.3. *Zrušenie certifikátov*

Digitálne certifikáty vo všeobecnosti môže zrušiť ich vystavujúca certifikačná autorita pomocou zoznamov zrušených certifikátov alebo odpovedajúceho subjektu protokolu OCSP (Online Certificate Status Protocol). CSCA pre systém DCC by mali poskytnúť zoznamy zrušených certifikátov (ďalej len „CRL“). Aj keď tieto CRL v súčasnosti iné členské štáty nevyužívajú, mali by sa začleniť pre budúce použitie. V prípade, že sa CSCA rozhodne neposkytnúť CRL, certifikáty DSC tohto CSCA sa musia obnoviť, keď sa CRL stanú povinnými. Overovatelia by nemali využívať protokol OCSP na validáciu DSC a mali by využívať CRL. Odporúča sa, aby vnútroštátny spracovateľský subjekt vykonal potrebnú validáciu certifikátov DSC stiahnutých z brány DCC a vnútroštátnym validátorom DCC poslal len súbor dôveryhodných a validovaných DSC. Validátori DCC by vo svojom procese validácie nemali vykonávať kontrolu zrušenia DSC. Jedným z dôvodov je ochrana súkromia držiteľov DCC, keďže sa predíde akejkoľvek možnosti, že by príslušný odpovedajúci subjekt protokolu OSCP mohol monitorovať použitie ktoréhokoľvek konkrétneho DSC.

Členské štáty môžu samy odstrániť svoje DSC z DCCG pomocou platných certifikátov na nahrávanie a certifikátov TLS. Odstránenie certifikátu DSC znamená, že všetky DCC vystavené s týmto DSC sa stanú neplatnými, keď členské štáty získajú aktualizované zoznamy DSC. Rozhodujúci význam má ochrana materiálu súkromných kľúčov zodpovedajúcich DSC. Členské štáty musia informovať prevádzkovateľa DCCG, ak musia zrušiť certifikáty na nahrávanie alebo certifikáty TLS, napríklad v dôsledku narušenia vnútroštátneho spracovateľského subjektu. Prevádzkovateľ DCCG môže potom odstrániť dôveru voči dotknutému certifikátu, a to napríklad jeho odstránením z bielej listiny TLS. Prevádzkovateľ DCCG môže odstrániť certifikáty na nahrávanie z databázy DCCG. Balíky podpísané súkromným kľúčom zodpovedajúcim tomuto certifikátu na nahrávanie sa stanú neplatnými, keď vnútroštátne spracovateľské subjekty odstránia dôveru voči zrušenému certifikátu na nahrávanie. Ak sa musí zrušiť certifikát CSCA, členské štáty informujú prevádzkovateľa DCCG, ako aj ostatné členské štáty, s ktorými majú vzťah dôvery. Prevádzkovateľ DCCG vystaví nový dôveryhodný zoznam, v ktorom sa už dotknutý certifikát nebude uvádzať. Všetky DSC vystavené týmto CSCA sa stanú neplatnými, keď členské štáty aktualizujú svoje úložisko vzťahov dôvery vnútroštátneho spracovateľského subjektu. V prípade, že sa musí zrušiť certifikát $DCCG_{TLS}$ alebo certifikát $DCCG_{TA}$, prevádzkovateľ DCCG a členské štáty musia spolupracovať na vytvorení nového dôveryhodného spojenia TLS a dôveryhodného zoznamu.

5. **Vzory certifikátov**

V tomto oddiele sa stanovujú kryptografické požiadavky a usmernenie, ako aj požiadavky na vzory certifikátov. V prípade certifikátov DCCG sa v tomto oddiele vymedzujú vzory certifikátov.

5.1. *Kryptografické požiadavky*

Kryptografické algoritmy a šifrovacie balíky TLS sa zvolia na základe aktuálneho odporúčania nemeckého Federálneho úradu pre bezpečnosť informácií (BSI) alebo organizácie SOG-IS. Tieto odporúčania a odporúčania iných inštitúcií a normalizačných organizácií sú podobné. Odporúčania možno nájsť v technických usmerneniach TR 02102-1 a TR 02102-2 ([1]) alebo dohodnutých kryptografických mechanizmoch SOG-IS ([2]).

5.1.1. Požiadavky na DSC

Uplatňujú sa požiadavky stanovené v *oddiele 3.2.2 prílohy I*. Dôrazne sa preto odporúča, aby podpisovatelia dokumentov využili algoritmus digitálneho podpisu na báze eliptických kriviek (ECDSA) s NIST-p-256 (ako sa vymedzuje v prílohe D k dokumentu FIPS PUB 186-4). Iné eliptické krivky sa nepodporujú. V dôsledku obmedzení veľkosti DCC by členské štáty nemali využívať algoritmus RSA-PSS, hoci je povolený ako záložný algoritmus.

([1]) BSI – Technické usmernenia TR-02102 (bund.de).
([2]) SOG-IS – Podporné dokumenty (sogis.eu).

V prípade, že členské štáty využívajú algoritmus RSA-PSS, mali by využiť veľkosť modulu 2048 alebo max. 3072 bitov. Pre podpis DSC sa ako kryptografická hašovacia funkcia použije SHA-2 s dĺžkou výstupu ≥ 256 bitov (pozri ISO/IEC 10118-3:2004).

5.1.2. Požiadavky na certifikáty TLS, certifikáty na nahrávanie a certifikáty CSCA

V prípade digitálnych certifikátov a kryptografických podpisov v kontexte DCCG sú hlavné požiadavky na kryptografické algoritmy a dĺžku kľúča zhrnuté v tejto tabuľke (pre rok 2021):

Algoritmus podpisu	Veľkosť kľúča	Hašovacia funkcia
EC-DSA	min. 250 bitov	SHA-2 s dĺžkou výstupu ≥ 256 bitov
RSA-PSS (odporúčaný padding) RSA-PKCS#1 v1.5 (legacy padding)	RSA modul (N) min. 3000 bitov s verejným exponentom e > 2^16	SHA-2 s dĺžkou výstupu ≥ 256 bitov
DSA	prvočíslo p min. 3000 bitov, kľúč q 250 bitov	SHA-2 s dĺžkou výstupu ≥ 256 bitov

Odporúčaná eliptická krivka pre EC-DSA je NIST-p-256, a to pre jej rozšírenú implementáciu.

5.2. *Certifikát CSCA (NB_{CSCA})*

V nasledujúcej tabuľke sa uvádza usmernenie o vzore certifikátu NB_{CSCA}, ak sa členský štát rozhodne pre systém DCC prevádzkovať vlastný CSCA.

Hrubo vytlačené položky sa vyžadujú (musia sa začleniť do certifikátu), položky označené *kurzívou* sa odporúčajú (mali by sa začleniť). Pri chýbajúcich poliach nie je vymedzené žiadne odporúčanie.

Pole	Hodnota
Subjekt	**cn=<neprázdny a jedinečný všeobecný názov>,***o=<poskytovateľ>,* **c=<členský štát prevádzkujúci CSCA>**
Používanie kľúča	**podpísanie certifikátu,***podpísanie CRL* (minimálne)
Základné obmedzenia	**CA = pravda, obmedzenia dĺžky cesty = 0**

Názov predmetu musí byť neprázdny a jedinečný v rámci špecifikovaného členského štátu. Kód krajiny c) musí zodpovedať členskému štátu, ktorý bude používať tento certifikát CSCA. Certifikát musí obsahovať jedinečný identifikátor kľúča subjektu (SKI) podľa dokumentu RFC 5280 ([3]).

5.3. *Certifikát podpisovateľa dokumentov (DSC)*

V nasledujúcej tabuľke sa poskytuje usmernenie k certifikátu DSC. **Hrubo vytlačené** položky sa vyžadujú (musia sa začleniť do certifikátu), položky označené *kurzívou* sa odporúčajú (mali by sa začleniť). Pri chýbajúcich poliach nie je vymedzené žiadne odporúčanie.

Pole	Hodnota
Sériové číslo	**jedinečné sériové číslo**
Subjekt	**cn=<neprázdny a jedinečný všeobecný názov>,***o=<poskytovateľ>,* **c=<členský štát, ktorý využíva tento DSC>**
Používanie kľúča	**digitálny podpis** (minimálne)

([3]) rfc5280 (ietf.org).

DSC musí byť podpísaný súkromným kľúčom zodpovedajúcim certifikátu CSCA, ktorý používa členský štát.

Použijú sa tieto rozšírenia:

— certifikát musí obsahovať identifikátor kľúča autority (AKI) zodpovedajúci identifikátoru kľúča subjektu (SKI) certifikátu vystavujúceho CSCA,

— certifikát by mal obsahovať jedinečný identifikátor kľúča subjektu (v súlade s dokumentom RFC 5280 ([4])).

Certifikát by mal okrem toho obsahovať rozšírenie distribučného bodu CRL odkazujúce na zoznam zrušených certifikátov (CRL) poskytnutý zo strany CSCA, ktorý vystavil DSC.

Certifikát DSC môže obsahovať rozšírenie pre rozšírené používanie kľúča s nula alebo viacerými identifikátormi politiky používania kľúča, ktoré obmedzujú typy potvrdení HCERT, ktoré možno pomocou tohto certifikátu overiť. Ak je prítomný jeden alebo viacero identifikátorov, overovatelia overia použitie kľúča na základe uloženého HCERT. Na to sú vymedzené tieto hodnoty extendedKeyUsage:

Pole	Hodnota
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.1 pre vystaviteľov potvrdenia o teste
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.2 pre vystaviteľov potvrdenia o očkovaní
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.3 pre vystaviteľov potvrdenia o prekonaní ochorenia

V prípade, že neexistuje žiadne rozšírenie pre používanie kľúčov (t. j. žiadne rozšírenia alebo nulové rozšírenia), je možné tento certifikát použiť na overenie akéhokoľvek typu HCERT. Príslušné doplnkové identifikátory politiky rozšíreného používania kľúča, ktoré sa používajú pri overovaní potvrdení HCERT, sa môžu vymedziť v iných dokumentoch.

5.4. *Certifikát na nahrávanie (NB_{UP})*

V nasledujúcej tabuľke sa poskytuje usmernenie pre certifikát vnútroštátneho spracovateľského subjektu na nahrávanie. **Hrubo vytlačené** položky sa vyžadujú (musia sa začleniť do certifikátu), položky označené *kurzívou* sa odporúčajú (mali by sa začleniť). Pri chýbajúcich poliach nie je vymedzené žiadne odporúčanie.

Pole	Hodnota
Subjekt	**cn=<neprázdny a jedinečný všeobecný názov>,** *o=<poskytovateľ>*,**c=<členský štát, ktorý používa tento certifikát na nahrávanie>**
Používanie kľúča	**digitálny podpis** (minimálne)

5.5. *Klientská autentifikácia TLS vnútroštátneho spracovateľského subjektu (NB_{TLS})*

V nasledujúcej tabuľke sa poskytuje usmernenie pre certifikát klientskej autentifikácie TLS vnútroštátneho spracovateľského subjektu. **Hrubo vytlačené** položky sa vyžadujú (musia sa začleniť do certifikátu), položky označené *kurzívou* sa odporúčajú (mali by sa začleniť). Pri chýbajúcich poliach nie je vymedzené žiadne odporúčanie.

Pole	Hodnota
Subjekt	**cn=<neprázdny a jedinečný všeobecný názov>,** *o=<poskytovateľ>*,**c=<členský štát vnútroštátneho spracovateľského subjektu>**
Používanie kľúča	**digitálny podpis** (minimálne)
Rozšírené používanie kľúča	**autentifikácia klienta (1.3.6.1.5.5.7.3.2)**

([4]) rfc5280 (ietf.org).

Certifikát môže obsahovať aj rozšírené používanie kľúča *serverová autentifikácia (1.3.6.1.5.5.7.3.1*), nie je to však povinné.

5.6. *Podpisový certifikát dôveryhodného zoznamu ($DCCG_{TA}$)*

V nasledujúcej tabuľke sa vymedzuje certifikát bodu dôvery DCCG.

Pole	Hodnota
Subjekt	**cn = Brána digitálneho zeleného osvedčenia** ([5])**, o=<poskytovateľ>, c=<krajina>**
Používanie kľúča	**digitálny podpis** (minimálne)

5.7. *Serverové certifikáty TLS pre DCCG ($DCCG_{TLS}$)*

V nasledujúcej tabuľke sa vymedzuje certifikát TLS DCCG.

Pole	Hodnota
Subjekt	cn=<FQDN alebo IP adresa DCCG>, o=<poskytovateľ>, c=<krajina>
SubjectAltName	dNSName: <názov DNS DCCG> alebo iPAddress: <IP adresa DCCG>
Používanie kľúča	**digitálny podpis** (minimálne)
Rozšírené používanie kľúča	**serverová autentifikácia (1.3.6.1.5.5.7.3.1**)

Certifikát môže obsahovať aj rozšírené používanie kľúča *klientská autentifikácia (1.3.6.1.5.5.7.3.2*), nie je to však povinné.

Certifikát TLS DCCG vystavuje verejne dôveryhodná certifikačná autorita (začlenená vo všetkých hlavných prehliadačoch a operačných systémoch v zmysle základných požiadaviek organizácie CA/Browser Forum).

([5]) V tejto súvislosti sa zachoval výraz „digitálne zelené osvedčenie“ namiesto výrazu „digitálny COVID preukaz EÚ“, keďže ide o terminológiu, ktorá bola pevne zakódovaná a využitá v potvrdení ešte pred tým, ako sa spoluzákonodarcovia rozhodli pre novú terminológiu.